US005982896A

United States Patent [19]

Cordery et al.

[11] Patent Number: 5,982,896

[45] Date of Patent: Nov. 9, 1999

[54] **SYSTEM AND METHOD OF VERIFYING CRYPTOGRAPHIC POSTAGE EVIDENCING USING A FIXED KEY SET**

[75] Inventors: **Robert A. Cordery**, Danbury; **David K. Lee**, Monroe; **Steven J. Pauly**, New Milford; **Leon A. Pintsov**, West Hartford; **Frederick W. Ryan, Jr.**, Oxford; **Monroe A. Welant, Jr.**, Trumbull, all of Conn.

[73] Assignee: **Pitney Bowes Inc.**, Stamford, Conn.

[21] Appl. No.: **08/772,739**

[22] Filed: **Dec. 23, 1996**

[51] **Int. Cl.**[6] **H04L 9/00**

[52] **U.S. Cl.** **380/21**; 380/23; 380/30; 380/45; 283/72; 283/73; 283/17

[58] **Field of Search** 380/3, 20, 21, 380/24, 25, 28, 29, 30, 44, 45, 47, 59; 235/431, 435, 470; 364/468.22, 478.03, 478.14, 478.15, 479.07, 601, 604, 704, 709.06; 283/69, 72, 73–75, 93, 113, 17; 178/79, 89

[56] **References Cited**

U.S. PATENT DOCUMENTS

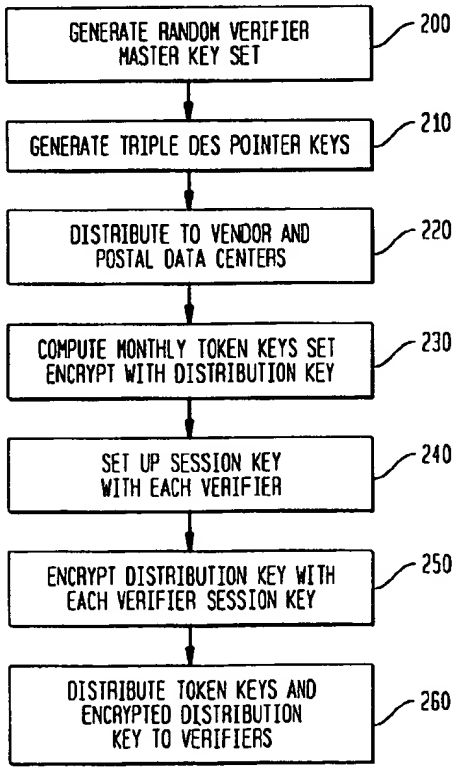
4,227,253	10/1980	Ehrsam et al.	375/2
4,238,853	12/1980	Ehrsam et al.	375/2
4,423,287	12/1983	Zeidler	178/22.08
4,850,017	7/1989	Matyas et al.	380/45
4,888,800	12/1989	Marshall et al.	380/21
5,142,577	8/1992	Pastor	380/21
5,231,666	7/1993	Matyas et al.	380/25
5,790,677	8/1998	Fox et al.	380/24

Primary Examiner—Tod R. Swann
Assistant Examiner—Paul E. Callahan
Attorney, Agent, or Firm—Charles R. Malandra, Jr.; Melvin J. Scolnick

[57] **ABSTRACT**

A method for controlling keys used in the verification of encoded information generated by a transaction evidencing device and printed on a document comprises the steps of generating a plurality of random verifier master keys to obtain a set of verifier master keys consisting of a fixed number of keys; generating at least one pointer by applying a psuedorandom algorithm to data unique to the transaction evidencing device; calculating a plurality of verifier token keys to obtain a verifier token key set corresponding to the set of verifier master keys; encrypting the verifier token key set with a privacy key; and distributing the set verifier token keys and the privacy key to verifiers. The token keys are a function of the verifier master keys and a code valid for a limited time. The pointer algorithm is an appropriate symmetric key cryptographic algorithm and the code is function of a date dependent parameter. The master keys are distributed to postal and vendor data centers.

5 Claims, 4 Drawing Sheets



US005878136A

United States Patent [19]

Kim et al.

[11] Patent Number: 5,878,136

[45] Date of Patent: Mar. 2, 1999

[54] **ENCRYPTION KEY CONTROL SYSTEM FOR MAIL PROCESSING SYSTEM HAVING DATA CENTER VERIFICATION**

[75] Inventors: **Hyung-Kun Paul Kim**, Wilton; **Robert A. Cordery**, Danbury; **Leon A. Pintsov**, West Hartford, all of Conn.

[73] Assignee: **Pitney Bowes Inc.**, Stamford, Conn.

[21] Appl. No.: **133,416**

[22] Filed: **Oct. 8, 1993**

[51] **Int. Cl.**[6] **H04L 9/00**

[52] **U.S. Cl.** **380/21**; 380/51; 380/55; 705/401; 705/405

[58] **Field of Search** 380/21, 23, 25, 380/51, 55; 364/464.02; 705/401-411

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,097,093	6/1978	Shelby et al.	305/22
4,097,923	6/1978	Eckert, Jr. et al.	364/900
4,376,299	3/1983	Rivest	380/51
4,649,266	3/1987	Eckert	235/432
4,725,718	2/1988	Sansone et al.	235/495
4,743,747	5/1988	Fougere et al.	235/494
4,757,537	7/1988	Edelmann et al.	380/51
4,775,246	10/1988	Edelmann et al.	380/23
4,807,139	2/1989	Liechti	364/464.02
4,873,645	10/1989	Hunter et al.	364/464.02
5,008,827	4/1991	Sansone et al.	364/464.02
5,142,577	8/1992	Pastor	380/21
5,170,044	12/1992	Pastor	235/454
5,202,922	4/1993	Iijima	380/21 X
5,243,654	9/1993	Hunter	380/51

FOREIGN PATENT DOCUMENTS

0376573	7/1990	European Pat. Off.	364/464.02
225210	1/1992	United Kingdom	G07B 17/00

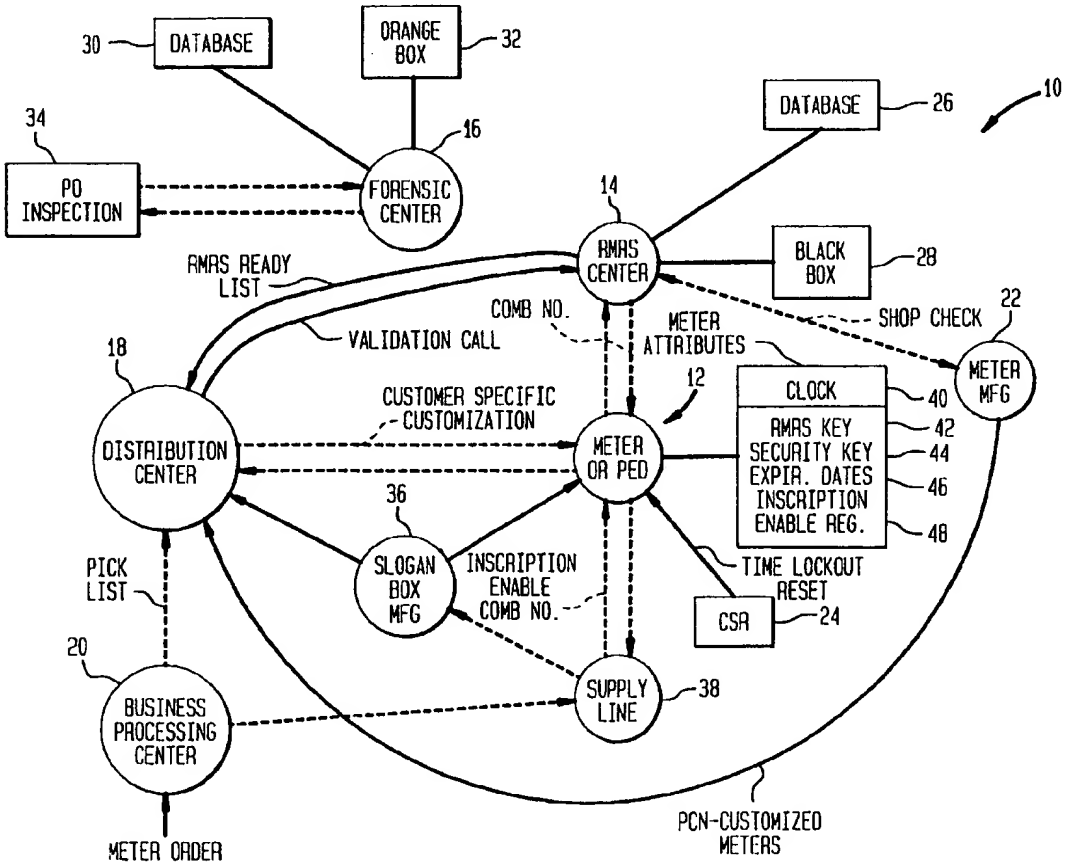
Primary Examiner—Bernarr Earl Gregory

Attorney, Agent, or Firm—Charles R. Malandra, Jr.; David E. Pitchenik; Melvin J. Scolnick

[57] **ABSTRACT**

A key control system comprises the generation of a first set of keys which are then used for a plurality of respective postage meters. The keys are then related to a respective meter in accordance with a map or algorithm. The keys may be changed by entering the second key via an encryption using the first key.

7 Claims, 7 Drawing Sheets



US005805701A

United States Patent [19]

Ryan, Jr.

[11] Patent Number: 5,805,701

[45] Date of Patent: Sep. 8, 1998

[54] ENHANCED ENCRYPTION CONTROL SYSTEM FOR A MAIL PROCESSING SYSTEM HAVING DATA CENTER VERIFICATION

[75] Inventor: Frederick W. Ryan, Jr., Oxford, Conn.

[73] Assignee: Pitney Bowes Inc., Stamford, Conn.

[21] Appl. No.: 742,526

[22] Filed: Nov. 1, 1996

[51] Int. Cl.[6] H04L 9/00

[52] U.S. Cl. 380/21

[58] Field of Search 380/21, 23, 49, 380/55

[56] References Cited

U.S. PATENT DOCUMENTS

4,757,532	7/1988	Gilham	380/21
4,853,961	8/1989	Pastor	380/21
4,893,338	1/1990	Pastor	380/21
5,696,829	12/1997	Cordery et al.	380/21

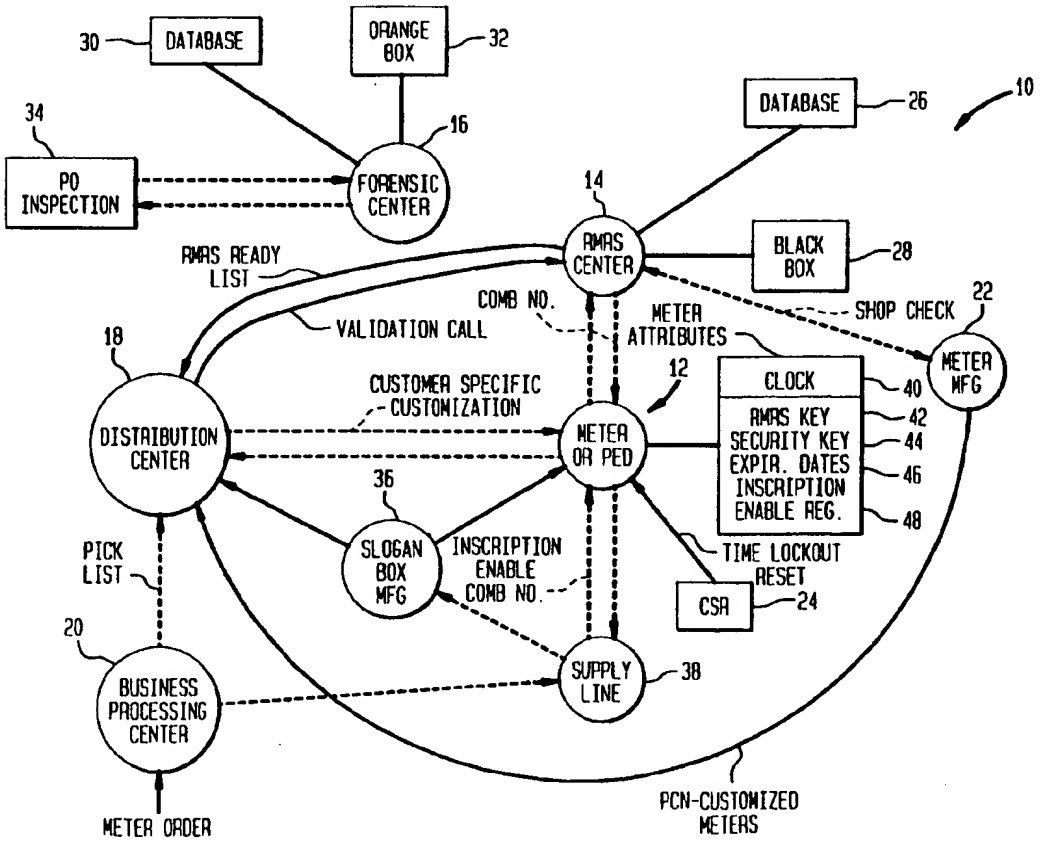
Primary Examiner—David Cain

Attorney, Agent, or Firm—Charles R. Malandra, Jr.; Melvin J. Scolnick

[57] ABSTRACT

A key control system comprises the generation of a first set of predetermined keys K_{pred} which are then used as master keys for a plurality of respective postage meters. The keys are then related to a respective meter in accordance with a map or algorithm. The predetermined master key K_{pred} is encrypted with the date to yield a date dependent key K_{dd} related to the respective meter. The date dependent key is encrypted with a unique identifier or the respective meter to yield a unique key K_{final} that is by the respective meter to generate digital tokens. The Data Center encrypts the date with each predetermined key K_{pred} to yield a table of dependent keys K_{dd}'s. The table of K_{dd}'s are distributed to verification sites. The verification site reads a meter's identification from a mailpiece being verified to obtain the dependent key K_{dd} of the meter. The verification site encrypts the dependent key K_{dd} with the unique identifier to obtain the unique meter key which is used to verify tokens generated by the meter. In the preferred embodiment, the master key K_{pred}, the date dependent key K_{dd}, and the unique key K_{final}, in the meter are stored in the meter. In an alternate embodiment, the master key K_{pred} is encrypted with a unique meter identifier to obtain and the unique key K_{final} which is stored in the meter. The meter then generates its date dependent key$_{dd}$, which is used to generate digital tokens.

8 Claims, 6 Drawing Sheets



US005742682A

United States Patent [19]

Baker et al.

[11] Patent Number: 5,742,682

[45] Date of Patent: Apr. 21, 1998

[54] **METHOD OF MANUFACTURING SECURE BOXES IN A KEY MANAGEMENT SYSTEM**

[75] Inventors: **Walter J. Baker**, Stratford; **Robert A. Cordery**, Danbury; **Frank M. D'Ippolito**, Derby; **Gary M. Heiden**, Shelton; **Kathyrn V. Lawton**, Branford; **Steven J. Pauly**, New Milford, all of Conn.

[73] Assignee: **Pitney Bowes Inc.**, Stamford, Conn.

[21] Appl. No.: **551,934**

[22] Filed: **Oct. 23, 1995**

Related U.S. Application Data

[63] Continuation of Ser. No. 414,897, Mar. 31, 1995, abandoned.

[51] **Int. Cl.**[6] **H04L 9/30**; G07B 17/04

[52] **U.S. Cl.** **380/21**; 380/25; 380/30

[58] **Field of Search** 380/21, 30, 23, 380/48, 4, 16, 25, 51, 55

[56] **References Cited**

U.S. PATENT DOCUMENTS

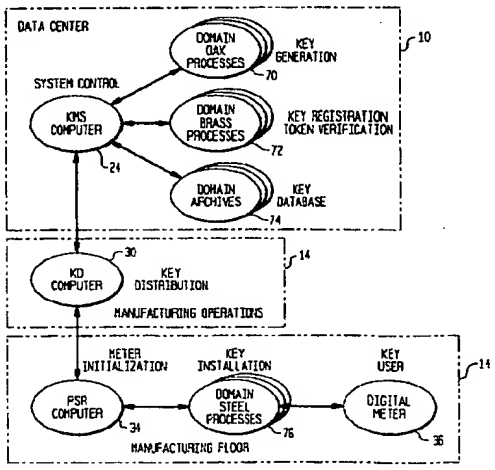
4,227,253	10/1980	Ehrsam et al.	375/2
4,238,853	12/1980	Ehrsam et al.	375/2
4,281,216	7/1981	Hogg et al.	178/22
4,578,531	3/1986	Everhart et al.	178/22
4,590,470	5/1986	Koenig	340/825
4,731,840	3/1988	Miniszewski et al.	380/21
4,850,017	7/1989	Matyas et al.	380/21
4,888,800	12/1989	Marshall et al.	380/21
4,888,801	12/1989	Foster et al.	380/21
4,888,802	12/1989	Cooney	380/49
4,956,863	9/1990	Goss	380/30
4,965,804	10/1990	Trbovich et al.	380/21
4,972,472	11/1990	Brown	380/21
5,016,277	5/1991	Hamilton	380/49
5,029,206	7/1991	Marino et al.	380/4
5,048,087	9/1991	Trbovich et al.	380/43
5,107,455	4/1992	Haines et al.	380/23
5,148,481	9/1992	Abrahamm et al.	380/46
5,173,938	12/1992	Steinbrenner	380/21
5,200,999	4/1993	Matyas et al.	380/25
5,214,698	5/1993	Smith	380/21
5,237,611	8/1993	Rasmussen et al.	380/21
5,241,599	8/1993	Bellovin	380/21
5,245,658	9/1993	Bush	380/20
5,247,576	9/1993	Bright	380/21
5,265,164	11/1993	Matyas et al.	380/30
5,301,231	4/1994	Abraham et al.	380/4
5,325,433	6/1994	Torii et al.	380/30
5,341,426	8/1994	Barney et al.	380/21
5,341,427	8/1994	Hardy et al.	380/21
5,390,251	2/1995	Pastor et al.	380/21
5,402,490	3/1995	Mihm, Jr.	380/21

Primary Examiner—Gilbert Barron, Jr.
Attorney, Agent, or Firm—Charles R. Malandra, Jr.; Melvin J. Scolnick

[57] **ABSTRACT**

A method of manufacturing a secure box in a Key Management System that includes a plurality of functionally distinct secure boxes initializes a first manufacturing box if one does not exist. The method creates in a manufacturing box at least one logical security domain including encryption keys needed to perform Key Management System processes within the domain, and provides a target secure box with the capability to perform at least one Key Management System function from a plurality of functions required by the Key Management System. The method authenticates the target secure box to the manufacturing box, installs a unique secure box identification in the target secure box, and creates at least one logical security domain in the target secure box corresponding to a logical security domain in the manufacturing box. The method sends a command from a Key Management System computer to initialize the target secure box to perform a domain process for at least one of Key Management System functions provided within the target secure box, and initializes the target secure box in each domain process indicated in the command from the Key Management System computer. The method installs in the target secure box the encryption keys required to perform a key generation process within the domain. For example, target secure box may be provided with at least one of a key verification function, a key installation function, a token verification function, a key registration function, or a secure box manufacturing function.

8 Claims, 16 Drawing Sheets



US005680456A

United States Patent [19]

Baker et al.

[11] Patent Number: 5,680,456

[45] Date of Patent: Oct. 21, 1997

[54] **METHOD OF MANUFACTURING GENERIC METERS IN A KEY MANAGEMENT SYSTEM**

[75] Inventors: **Walter J. Baker**, Stratford; **Feliks Bator**, Easton; **Robert A. Cordery**, Danbury; **Frank M. D'Ippolito**, Derby; **Kevin D. Hunter**, Stratford; **Kathryn V. Lawton**, Branford; **David K. Lee**, Monroe; **Louis J. Logliscl**, Stamford; **Steven J. Pauly**, New Milford; **Leon A. Pintsov**, West Hartford; **Ian A. Siveyer**, Monroe, all of Conn.

[73] Assignee: **Pitney Bowes Inc.**, Stamford, Conn.

[21] Appl. No.: **415,824**

[22] Filed: **Mar. 31, 1995**

[51] **Int. Cl.**[6] **H04L 9/08**; H04L 9/00; G06F 17/00

[52] **U.S. Cl.** **380/21**; 380/23; 380/25; 380/49; 364/464.11; 364/464.15

[58] **Field of Search** 380/21, 23, 24, 380/25, 30, 46, 49, 50, 51, 59; 364/464.02, 464.11–464.19, 464.2, 464.4

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,227,253	10/1980	Ehrsam et al. .	
4,238,853	12/1980	Ehrsam et al. .	
4,281,216	7/1981	Hogg et al. .	
4,578,531	3/1986	Everhart et al. .	
4,590,470	5/1986	Koenig .	
4,731,840	3/1988	Miniszewski et al.	380/21
4,850,017	7/1989	Matyas et al.	380/21
4,888,800	12/1989	Marshall et al.	380/21
4,888,801	12/1989	Foster et al.	380/21
4,888,802	12/1989	Cooney	380/49
4,916,738	4/1990	Chandra et al.	380/25
4,956,863	9/1990	Goss	380/30
4,965,804	10/1990	Trbovich et al.	380/21
4,972,472	11/1990	Brown	380/21
5,016,277	5/1991	Hamilton	380/49
5,029,206	7/1991	Marino et al.	380/4
5,048,087	9/1991	Trbovich et al.	380/43
5,148,481	9/1992	Abrahamm et al.	380/46
5,173,938	12/1992	Steinbrenner et al.	380/21
5,200,999	4/1993	Matyas et al.	380/25
5,214,698	5/1993	Smith	380/21
5,237,611	8/1993	Rasmussen et al.	380/21
5,241,599	8/1993	Bellovin	380/21
5,245,658	9/1993	Bush	380/20
5,247,576	9/1993	Bright	380/21
5,265,164	11/1993	Matyas et al.	380/30
5,325,433	6/1994	Tonii et al.	380/30
5,341,426	8/1994	Barney et al.	380/21
5,341,427	8/1994	Hardy et al.	380/21

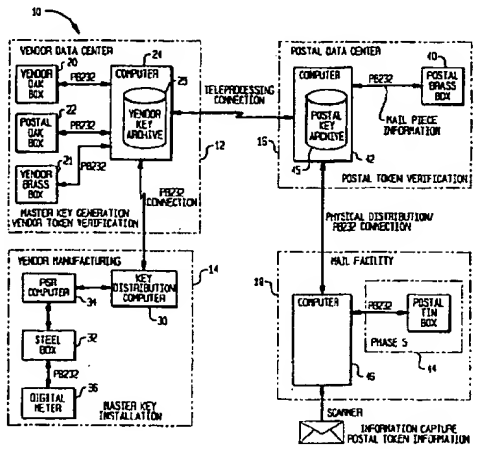
Primary Examiner—Bernarr E. Gregory

Attorney, Agent, or Firm—Charles R. Malandra, Jr.; David E. Pitchenik; Melvin J. Scolnick

[57] **ABSTRACT**

A method of manufacturing transaction evidencing devices, such as digital postage meters, includes the steps of generating a master key in a logical security domain of a Key Management System; installing the master key into a digital postage meter; verifying the installation of the master key; and registering the master key to a logical security sub-domain in the Key Management System. The step of generating the master key further includes the steps of generating a domain; generating at least one sub-domain; installing the domain in secure boxes of the Key Management System; generating a master key and test token within the domain; and recording the master key in the domain archive. The step of installing the master key further includes the steps of installing the master key into a digital meter; and associating the master key with a unique device identifier. The step of registering the master key to a logical security sub-domain in the Key Management System further includes the steps of assigning a sub-domain to the digital meter; installing a postal identifier into the digital meter; associating the postal identifier to the unique device identifier; generating a registration token in the digital meter based on the postal identifier and the unique device identifier; generating registration tokens using the master key recorded in the archives; verifying that the registration tokens are identical; and recording the master key in the sub-domain. The steps are repeated for each domain assigned to the digital postage meter.

15 Claims, 16 Drawing Sheets



US005661803A

United States Patent [19]

Cordery et al.

[11] Patent Number: 5,661,803

[45] Date of Patent: Aug. 26, 1997

[54] **METHOD OF TOKEN VERIFICATION IN A KEY MANAGEMENT SYSTEM**

[75] Inventors: **Robert A. Cordery**, Danbury; **John F. Braun**, Weston; **Frank M. D'Ippolito**, Derby; **Kathyrn V. Lawton**, Branford; **Steven J. Pauly**, New Milford; **Leon A. Pintsov**, West Hartford; **Frederick W. Ryan, Jr.**, Oxford; **Monroe A. Weiant, Jr.**, Trumbull, all of Conn.

[73] Assignee: **Pitney Bowes Inc.**, Stamford, Conn.

[21] Appl. No.: **414,896**

[22] Filed: **Mar. 31, 1995**

[51] **Int. Cl.**[6] **H04L 9/00**; H04L 9/08

[52] **U.S. Cl.** **380/21**; 380/23; 380/24; 380/25; 380/49

[58] **Field of Search** 380/9, 21, 23, 380/24, 25, 44, 46, 49, 50

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,227,253	10/1980	Ehrsam et al.	380/45
4,238,853	12/1980	Ehrsam et al.	380/45
4,281,216	7/1981	Hogg et al.	380/23
4,578,531	3/1986	Everhart et al.	380/21
4,590,470	5/1986	Koenig	380/23
4,731,840	3/1988	Miniszewski et al.	380/21
4,850,017	7/1989	Matyas et al.	380/21
4,888,800	12/1989	Marshall et al.	380/21
4,888,801	12/1989	Foster et al.	380/21
4,888,802	12/1989	Cooney	380/49
4,956,863	9/1990	Goss	380/30
4,965,804	10/1990	Trbovich et al.	380/21
4,972,472	11/1990	Brown	380/21
5,016,277	5/1991	Hamilton	380/49
5,029,206	7/1991	Marino et al.	380/4
5,048,087	9/1991	Trbovich et al.	380/43
5,138,712	8/1992	Corbin	380/23 X
5,148,481	9/1992	Abrahamm et al.	380/46
5,173,938	12/1992	Steinbrenner	380/21
5,200,999	4/1993	Matyas et al.	380/25
5,214,698	5/1993	Smith	380/21
5,237,611	8/1993	Rasmussen et al.	380/21
5,241,599	8/1993	Bellovin	380/21
5,245,658	9/1993	Bush	380/20
5,247,576	9/1993	Bright	360/21
5,265,164	11/1993	Matyas et al.	380/30
5,325,433	6/1994	Torii et al.	380/30
5,341,426	8/1994	Barney et al.	380/21
5,341,427	8/1994	Hardy et al.	380/21
5,454,038	9/1995	Cordery et al.	380/23
5,491,752	2/1996	Kaufman et al.	380/25 X
5,506,961	4/1996	Carlson et al.	380/25 X

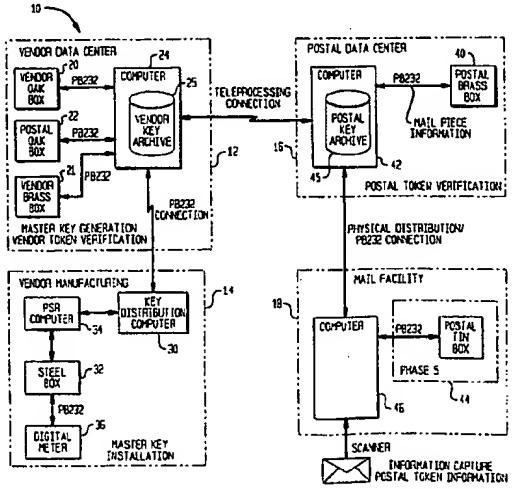
Primary Examiner—Bernar E. Gregory

Attorney, Agent, or Firm—Charles R. Malandra, Jr.; David E. Pitchenik; Melvin J. Scolnick

[57] **ABSTRACT**

A method of token verification in a Key Management System provides a logical device identifier and a master key created in a logical security domain to a transaction evidencing device, such as a digital postage meter. The method creates a master key record in a key verification box, securely stores the master key record in a Key Management System archive, and produces in the transaction evidencing device evidence in the logical security domain of transaction information integrity. The method inputs the evidence of the transaction information integrity to a token verification box, and inputs in the token verification box the master key record from the Key Management System archive. The method determines in the token verification box that the master key is valid in logical security domain, uses in the token verification box the master key to verify the evidence of transaction information integrity, and outputs from the token verification box an indication of the result of the verification of the evidence of transaction information integrity. The master key record includes the logical device identifier, the master key and a digital signature associating the logical device identifier and the master key. The method checks the digital signature to verify the association of the logical device identifier and the master key within the logical security domain.

14 Claims, 16 Drawing Sheets



United States Patent [19]

Pastor

[11] **Patent Number: 4,853,961**

[45] **Date of Patent: Aug. 1, 1989**

[54] **RELIABLE DOCUMENT AUTHENTICATION SYSTEM**

[75] Inventor: **Jose Pastor**, Westport, Conn.

[73] Assignee: **Pitney Bowes Inc.**, Stamford, Conn.

[21] Appl. No.: **136,251**

[22] Filed: **Dec. 18, 1987**

[51] **Int. Cl.**[4] **H04L 9/00**

[52] **U.S. Cl.** **380/21**; 380/25; 380/30

[58] **Field of Search** 380/21, 30, 25

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,438,824	3/1984	Mueller-Schloer	380/30
4,458,109	7/1984	Mueller-Schloer	380/30
4,723,284	2/1988	Munck et al.	380/30
4,731,841	3/1988	Rosen et al.	380/30
4,759,063	7/1988	Chaum	380/30
4,759,064	7/1988	Chaum	380/30

FOREIGN PATENT DOCUMENTS

132782	7/1984	European Pat. Off. .
214609	9/1986	European Pat. Off. .
2100190	6/1982	United Kingdom .
2140179	5/1983	United Kingdom .
2164181	8/1986	United Kingdom .

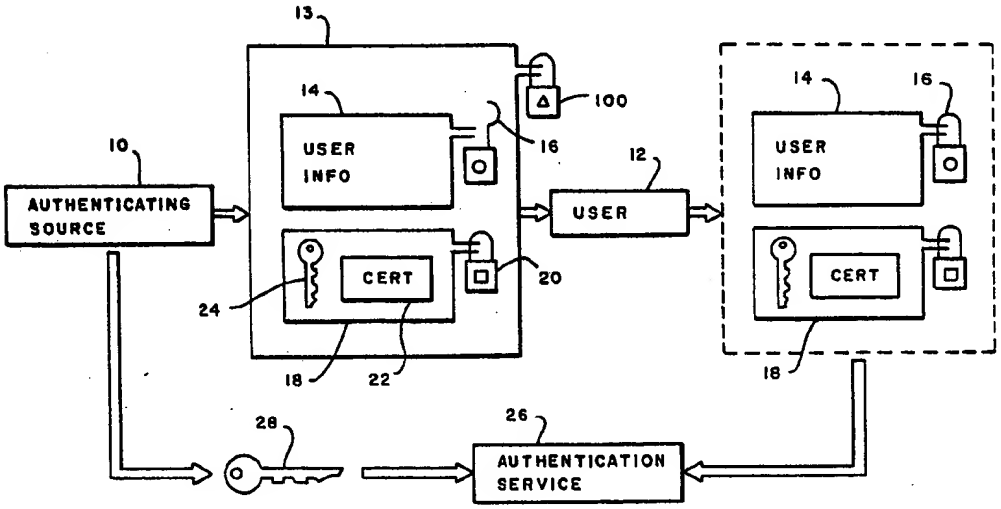
Primary Examiner—Salvatore Cangialosi

Attorney, Agent, or Firm—Robert H. Whisker; Melvin J. Scolnick; David E. Pitchenik

[57] **ABSTRACT**

A system for reliably authenticating a document includes a device having a decryption key therein that, upon application to information provided by a user, reveals not only a plain text message indicating the source of the authentication but, in addition, provides the decryption key for use with the information provided by the mailer.

17 Claims, 2 Drawing Sheets



	Type	L #	Hits	Search Text	DBs	Time Stamp
1	IS&R	L1	2	(("5737419") or ("5867578")).PN.	USPAT	2001/08/02 14:08
2	BRS	L2	1190	(certify or certifying or certificate) and (public or private or secret) and (key or keys) and (fragment or count or piececount or date or meter or value or amount or weight or size or register or zip or zipcode or (delivery near control near code) or (piece near count))	USPAT	2001/08/02 14:40
3	IS&R	L4	7	(("4853961") or ("5661803") or ("5680456") or ("5742682") or ("5805701") or ("5878136") or ("5982896")).PN.	USPAT	2001/08/02 14:12
4	BRS	L5	246	2 and (postal or postage or frank or franking or meter or metering)	USPAT	2001/08/02 14:43
5	BRS	L6	329	2 and (indicium or indicia or mark or postage)	USPAT	2001/08/02 14:44
6	BRS	L7	147	5 and signature	USPAT	2001/08/02 14:44
7	BRS	L8	185	6 and signature	USPAT	2001/08/02 15:11
8	BRS	L9	137	7 and (verify or verification or verifying)	USPAT	2001/08/02 15:11
9	BRS	L10	174	8 and (verify or verification or verifying)	USPAT	2001/08/02 15:11

	Document ID	Issue Date	Current OR	Inventor
1	US 5982896 A	19991109	705/62	Cordery, Robert A. , et al.
2	US 5878136 A	19990302	705/60	Kim, Hyung-Kun Paul , et al.
3	US 5805701 A	19980908	705/60	Ryan, Jr., Frederick W.
4	US 5742682 A	19980421	380/277	Baker, Walter J. , et al.
5	US 5680456 A	19971021	705/71	Baker, Walter J. , et al.
6	US 5661803 A	19970826	705/60	Cordery, Robert A. , et al.
7	US 4853961 A	19890801	713/176	Pastor, Jose